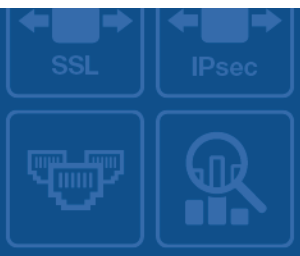
FORTINET
High Performance Network Security

FortiOS™ Handbook - PCI DSS Compliance

VERSION 5.4.0



FORTIOS
5.4
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

February-03-16

FortiOS™ Handbook - PCI DSS Compliance

01-540-129720-20160203

TABLE OF CONTENTS

Change Log

Date	Change Description
February 3, 2016	Initial Release

Introduction

This document describes how FortiOS is compliant with Payment Card Industry Data Security Standard (PCI DSS).

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- FortiGuard Analysis & Management Service is properly configured.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

Configuring FortiGate units for PCI DSS compliance on page 8 explains the Payment Card Industry Data Security Standard (PCI DSS). It provides information about configuring your network and FortiGate unit to help you comply with PCI DSS requirements.

FortiOS 5.4 compliance and certification new features

Vulnerability Scanning has been removed (293156)

Vulnerability scanning can now be done from FortiClient.

PCI DSS Compliance Check Support (270014)

FortiOS 5.4 allows you to run a compliance check either on demand or according to a schedule that automatically checks PCI DSS compliance at the global or VDOM level. The compliance check determines whether the FortiGate is compliant with each PCI DSS requirement by displaying an 'X' next to the non-compliant entries in the GUI logs.

Go to **System > Advanced > Compliance**, turn on compliance checking and configure a daily time to run the compliance check. Or you can select **Run Now** to run the compliance check on demand.

Go to **Log & Report > Compliance Events** to view compliance checking log messages that show the results of running compliance checks.

#	Date/Time	Level	Message	Result
1	15:54:31		Check that all audit trails include date, time and user identification	
2	15:54:31		Check the dropped out-of-state ICMP packets are logged	
3	15:54:31		Check the dropped out-of-state TCP packets are logged	
4	15:54:31		Check that a message is displayed to locked out Administrators	
5	15:54:31		Check that Administrators' accounts are unlocked after 30 minutes	
6	15:54:31		Check that Administrators are locked out after 3 login failures	
7	15:54:31		Check that each Firewall rule has a Comment defined	
8	15:54:31		Check that each Firewall rule has a Name defined	

Configuring FortiGate units for PCI DSS compliance

This chapter provides information about configuring your network and FortiGate unit to help you comply with PCI DSS requirements. There is also some description of other Fortinet products that can help you with PCI DSS compliance.

Introduction to PCI DSS

The primary source of information for your PCI DSS compliance program is the Payment Card Industry (PCI) Data Security Standard itself. Version 3.1 of the standard was published in April 2015. The following is a brief summary of PCI DSS.

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) sets data handling requirements for organizations that hold, process, or exchange cardholder information.

What is the Cardholder Data Environment

Throughout the PCI DSS requirements, there are references to the Cardholder Data Environment (CDE). The CDE is the computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment.

PCI DSS objectives and requirements

PCI DSS consists of 7 control objectives and 12 requirements.

PCI DSS Control Objectives and Requirements

Control Objective	Requirement	Fortinet Solution
Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data	FortiGate firewall functionality. See Security policies for the CDE network on page 14
	2. Do not use vendor - supplied defaults for system passwords and other security parameters	FortiDB vulnerability assessment and auditing FortiWeb web application password checking See Password complexity and change requirements on page 20

Control Objective	Requirement	Fortinet Solution
Protect Cardholder Data	**3.** Protect stored cardholder data	FortiDB vulnerability assessment and monitoring FortiWeb web application firewall See Protecting stored cardholder data on page 17
	4. Encrypt transmission of cardholder data across open, public networks	FortiGate IPsec VPN. See Protecting communicated cardholder data on page 17
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update antivirus software or programs	FortiGate integrated AV FortiClient integrated AV FortiMobile integrated AV FortiMail integrated AV FortiGuard automated AV updates See Protecting the CDE network from viruses on page 18
	6. Develop and maintain secure systems and applications	FortiDB vulnerability assessment, auditing and monitoring FortiWeb web application security FortiGate Application Control
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need-to-know	FortiDB vulnerability assessment, auditing and monitoring. See Restricting access to cardholder data on page 20
	8. Identify and authenticate access to system components	FortiGate integrated database or hooks to Active Directory. See Controlling access to the CDE network on page 20
	9. Restrict physical access to cardholder data	Fortinet professional services in partnership with partner solutions

Control Objective	Requirement	Fortinet Solution
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data	FortiDB auditing and monitoring FortiAnalyzer event reporting See Monitoring the network for vulnerabilities.
	11. Regularly test security systems and processes	FortiDB vulnerability assessment See Monitoring the network for vulnerabilities.
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel	FortiManager security policy management appliance

This chapter describes how the FortiGate's features can help your organization to be compliant with PCI DSS. Requirements that the FortiGate cannot enforce need to be met through organization policies with some means determined for auditing compliance.

Be sure to read the following wireless guidelines. Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that wireless networking has not been introduced into the CDE.

Wireless guidelines

While wired networks usually connect fixed known workstations, wireless networks are more dynamic, introducing a different set of security concerns.

Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that unauthorized wireless networking has not been introduced into the CDE. Wireless networking could be introduced quite casually by adding a wireless device to a PC on the CDE network.

For all PCI DSS networks, whether they use wireless technology or not, the following requirement applies:

- Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. (11.1)

If your organization uses wireless networking outside the CDE network and the firewall prevents communication with the CDE network, the wireless network is outside the PCI DSS scope, but the firewall configuration must meet PCI DSS requirements.

If your organization uses wireless networking inside the CDE network, the wireless network is within the PCI DSS scope. For information about wireless network requirements, see Wireless network security on page 15.

Running PCI DSS compliance checks

FortiOS 5.4 allows you to run a compliance check either on demand or according to a schedule that automatically checks PCI DSS compliance at the global and/or VDOM level. The compliance check determines whether the

FortiGate is compliant with each PCI DSS requirement by displaying an 'X' next to the non-compliant entries in the GUI logs.

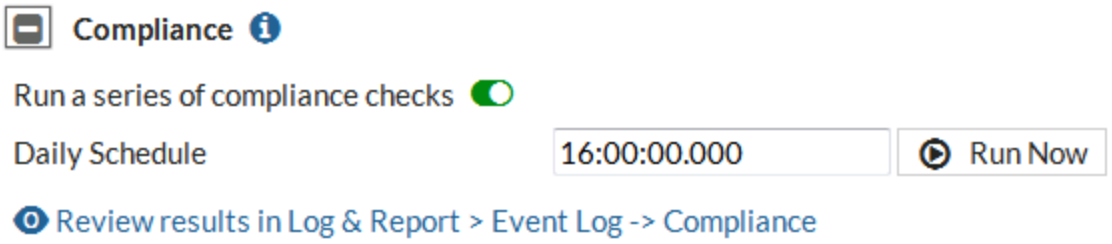
The FortiGate runs at least 50 compliance checks that report on the status of a number of things including:

- Checking that out of stet ICMP packets are dropped
- The TCP end timeout is set
- SSH and SSL deep inspection with web filtering drops traffic from servers with invalid server certificates
- Verifying that IPS signatures, Application Control signatures, and Antivirus signatures are up to date
- Determining if Spyware/Malicious sites are being blocked by a web filtering policy
- Verifying that administrators are locked out after 3 login failures

For a complete list of compliance checks go to **Log & Report > Compliance Events**.

Configuring PCI DSS compliance checking

Go to **System > Advanced > Compliance**, turn on compliance checking and configure a daily time to run the compliance check. Or you can select **Run Now** to run the compliance check on demand.



Go to **Log & Report > Compliance Events** to view compliance checking log messages that show the results of running compliance checks.

#	Date/Time	Level	Message	Result
1	15:54:31		Check that all audit trails include date, time and user identification	
2	15:54:31		Check the dropped out-of-state ICMP packets are logged	
3	15:54:31		Check the dropped out-of-state TCP packets are logged	
4	15:54:31		Check that a message is displayed to locked out Administrators	
5	15:54:31		Check that Administrators' accounts are unlocked after 30 minutes	
6	15:54:31		Check that Administrators are locked out after 3 login failures	
7	15:54:31		Check that each Firewall rule has a Comment defined	
8	15:54:31		Check that each Firewall rule has a Name defined	

You can also configure compliance checking and set up the schedule from the CLI:

```
config system global
   set compliance-check {disable| enable}
   set compliance-check-time <time>
end
```

Use the following command to run on-demand compliance checking:

```
execute dsscc
```

Per-VDOM compliance checking

If you have multiple VDOMs enabled compliance checking can be run separately for each VDOM.

Begin from the Global view by going to **System > Advanced > Compliance** and turning on compliance checking and configuring a daily time to run the compliance check. This compliance check daily schedule will be used to run compliance checks on individual VDOMs where compliance checking is enabled them.

You can also enable global compliance checking from the CLI:

```
config global
   config system global
      set compliance-check {disable| enable}
      set compliance-check-time <time>
   end
```

Then log onto each VDOM for which to enable compliance checking and go to to **System > Advanced > Compliance**, and turn on compliance checking . You can also select **Run Now** to run a compliance check on that VDOM on demand.

From the CLI edit a VDOM and use the following command to enable compliance checking for that VDOM. The following example shows how to enable compliance checking for the root VDOM:

```
config vdom
   edit root
      config system settings
         set compliance-check enable
      end
```

From the CLI you can also log into a VDOM and use the following command to run on-demand compliance checking:

```
execute dssccc
```

From a VDOM GUI go to **Log & Report > Compliance Events** to view compliance checking log messages that show the results of running compliance checks.

Compliance checking diagnose command

Use the following command to display diagnostic information about compliance checking:

```
diagnose debug application dssccd <debug_level>
```

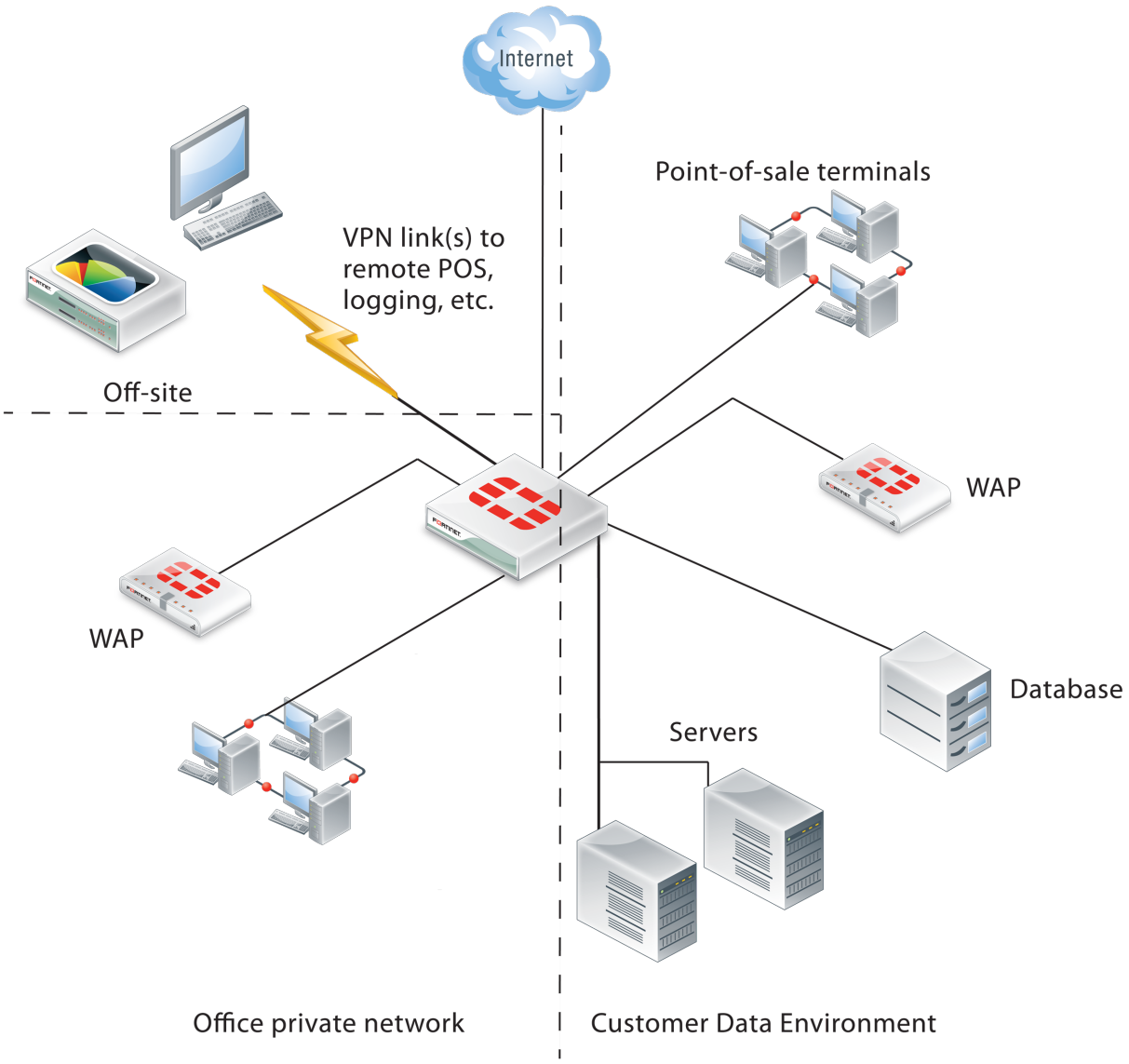
Network topology

The cardholder data environment must be protected against unauthorized access from the Internet and from other networks in your organization. FortiGate unit firewall functionality provides tight control over the traffic that can pass between the following network interfaces:

- Internet
- CDE wired LAN
- CDE wireless LAN
- Other internal networks

The figure below shows how the Cardholder Data Environment can be delineated in a typical network.

Enterprise network with a cardholder data environment



Internet

The FortiGate unit has at least one network interface connected to the Internet. If your organization uses more than one Internet service provider, there could be additional network interfaces that function as a route to the Internet.

The CDE wired LAN

The CDE network typically contains point-of-sale (POS) terminals, databases, and servers. The only security policies between the CDE network and the Internet should be for encrypted connections. For remote point-of-sale terminals or off-site databases, VPN connections are required and they should use strong encryption. For a web server that handles online purchases, only HTTPS (SSL or TLS) connections can be permitted. The security

policies that enable these connections should have the narrowest possible definitions for source address, destination address and service.

PCI DSS does not require the CDE network to be isolated from the rest of your corporate LAN. But isolating the CDE network reduces the scope of required data protection measures and may reduce the scope of PCI DSS assessments that are periodically required.

The CDE wireless LAN

Wireless networking is a special issue. Even if you do not use wireless technology you must monitor to ensure that unauthorized wireless access has not been added to the CDE network. For this purpose, the figure above shows a FortiAP device in the CDE. The FortiAP device can provide dedicated wireless monitoring, an access point, or both.

A small retail outlet could reduce costs by using a FortiWiFi unit, a FortiGate unit with integrated wireless networking. The FortiWiFi unit would have to be located where it could provide sufficient wireless monitoring (or access point) coverage for the entire premises.

Other internal networks

Other internal networks such as your office LAN, unless they provide connection to the CDE, are not subject to PCI DSS requirements.

Security policies for the CDE network

The FortiGate unit's firewall functionality is ideally suited to PCI DSS requirement 1.2.1, "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic." Security policies control the source, destination, and type of traffic passing between networks.

The PCI DSS standard includes requirements to document your network topology and configuration. As part of that requirement, and to assist the auditing of your network, make use of the **Comment** field available in FortiGate security policies. Describe the purpose of each policy.

Controlling the source and destination of traffic

The source and destination are the first parameters you specify in a security policy. (Go to **Policy & Objects > IPv4 Policy** and select **Create New**.)

The **Interface** settings depend on network topology. The **Source** and **Destination Address**settings define the IP addresses to which the policy applies. These should be as narrow as possible, so that only the appropriate hosts are included. For example, if the destination is a server with a single IP address, the named **Destination Address** should be defined as that single address, not the entire subnet on which the server resides.

Addresses are defined in **Policy & Objects > Addresses**. Some addresses will be used in several security policies, so it is best to plan ahead and define the addresses first.

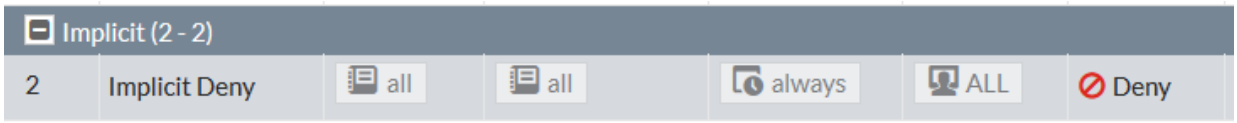
Controlling the types of traffic in the CDE

The **Policy & Objects > Service** setting determines which types of traffic can pass based on protocol.

You can select a single protocol from the **Service** drop-down list. To add another protocol, select the green "+" button to access the **Service** drop-down list again. If several security policies will need the same list of services, consider creating a named service group. (Go to **Firewall Objects > Service > Groups**.) In the security policy, service groups are available at the bottom of the **Service** drop-down list.

The default deny policy

All traffic not specifically allowed by a security policy that you create is blocked by the Implicit policy listed at the bottom of the **Policy & Objects > IPv4 Policy** page.



You cannot delete this policy and you can edit the policy only to enable or disable logging of the traffic that it handles.

Wireless network security

Scanning for rogue access points is the minimum requirement for wireless security. Even if your organization does not use wireless networking, PCI DSS requires you to verify periodically that wireless networking has not been introduced into the CDE.

If you use wireless networking, the wireless network is only within the PCI DSS scope if it can connect to the CDE.

On-wire detection of rogue APs

FortiGate units include an "on-wire" detection technique that correlates the SSID MAC addresses of the unknown access points with MAC addresses detected on your wired networks. This helps to differentiate unrelated neighboring APs from security-compromising unauthorized APs connected to your network.

Setting up rogue access point scanning

A FortiGate unit with a connected FortiAP unit can perform wireless scanning. Each of the FortiAP radios can act as a dedicated monitor or can perform scanning in the background while acting as a wireless access point.

Radio 1 operates in the 2.4GHz band and Radio 2 operates in the 5GHz band. Both bands should be monitored. The FortiAP unit(s) used for scanning must be located within the coverage area that would result if an access point were added to the CDE.

To configure rogue AP scanning in a FortiAP profile

1. Go to **WiFi Controller > WIDS Profiles**.
   On some models, the menu is **WiFi & Switch Controller**.
2. Select an existing WIDS profile and edit it, or select **Create New**.
3. Make sure that **Enable Rogue AP Detection** is selected.
4. Select **Enable On-Wire Rogue AP Detection**.
5. Optionally, enable **Auto Suppress Rogue APs in Foreground Scan**.
6. Select **OK**.

Viewing the results of rogue AP scanning

Go to **Monitor > Rogue AP Monitor** to view information about detected rogue wireless access points.

Logging the results of rogue AP scanning

To ensure that detection of rogue access points is logged, go to **Log & Report > Log Settings**, enable **Event Logging** and select **WiFi activity event**.

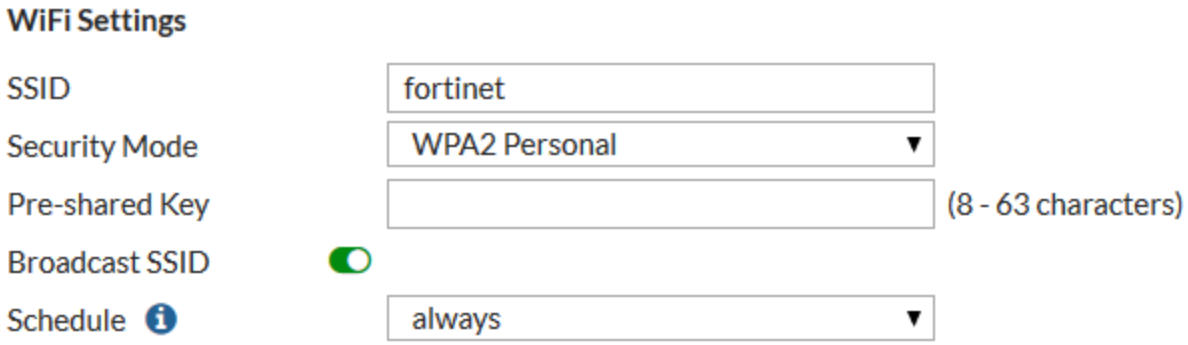
Securing a CDE network wireless access point

If your wireless network is within PCI DSS scope, it must meet the following requirements:

- Default settings such as SSID and passphrases must be changed.
- Use WPA/WPA2 security.
- Log wireless activity.

Setting wireless security

On FortiGate units, go to **WiFi Controller > SSID** to configure wireless security settings for either a new or existing virtual access point.



The default SSID for the FortiAP is “fortinet”. You must change this.

The **Security Mode** must be set to one of the WPA2 modes. Both WPA or WPA2 clients can be served. In the CLI, you can optionally select exclusively WPA or WPA2 operation.

WPA/WPA2-Enterprise **Authentication** uses separate logon credentials for each user. Either FortiGate user group security or an external RADIUS server performs the authentication. Optionally, certificate-based security can also be applied. WPA/WPA2-Personal authentication requires a single pre-shared key that is used by all clients and is thus less secure.

For detailed information about wireless access points, see the Deploying Wireless Networks chapter of the FortiOS Handbook.

Logging wireless network activity

To ensure that wireless network actiity is logged, go to **Log & Report > Log Settings**, enable **Event Logging** and select **WiFi activity event**.

Protecting stored cardholder data

The Fortinet FortiDB and FortiWeb products can provide security for your sensitive cardholder data.

The Fortinet Database Security (FortiDB) device provides vulnerability assessment, database activity monitoring, auditing and monitoring.

The Fortinet FortiWeb Web Application Firewall deployed in front of public-facing web applications protects Web applications, databases, and the information exchanged between them. In particular, it addresses the PCI DSS requirements 6.5 and 6.6 regarding web application vulnerabilities such as cross-site scripting, SQL injection, and information leakage.

FortiGates support some web application firewall security features and allow you to offload selected HTTP and HTTPS traffic to an external FortiWeb device. To offload HTTP traffic to go **System > External Security Devices,** enable **HTTP service** and select FortiWeb.

Protecting communicated cardholder data

If cardholder data must be communicated over an untrusted network, such as the Internet, use the FortiGate unit's IPsec VPN capability to exchange the data securely. If you support customer online transactions, use HTTPS (SSL or TLS encryption) for security. The relevant PCI DSS requirement is:

- Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. (4.1)

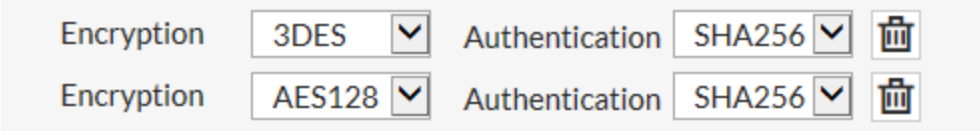
This does not prescribe particular cryptography, but it can be interpreted as a requirement to follow industry best practices.

Configuring IPsec VPN security

The security considerations for IPsec VPNs are encryption and authentication.

Encryption

Go to **VPN > IPsec Tunnels** to configure an IPsec VPN. In both Phase 1 and Phase 2 parts of the configuration, you select the encryption to use.



These are advanced settings, overriding defaults that are not necessarily the strongest algorithms. VPNs negotiate over standards, so you can list multiple proposed algorithms. The VPN will use the strongest encryption that both ends support.

Choose strong encryption. The available encryption algorithms in descending order of strength are AES256, AES192, AES128, 3DES, DES. DES encryption is the weakest with only a 64-bit key and does not meet the 80-bit key length minimum that PCI DSS requires.

The message digest (authentication) algorithms in descending order of strength are SHA512, SHA384, SHA256, SHA1 and MD5. MD5 is particularly weak and should be avoided.

Authentication

VPN peers authenticate each other before establishing a tunnel. FortiGate units support two different authentication methods: pre-shared key and RSA signature (certificate). Certificates provide the best security. PCI DSS does not prohibit pre-shared keys, but you should limit access to the keys to the personnel who are responsible for the FortiGate units or other equipment at either end of the VPN.

Configuring SSL VPN security

The SSL VPN configuration includes a choice of encryption algorithm. You can only configure encryption key algorithms for SSL VPN in the CLI:

```
config vpn ssl settings
   set algorithm {low | medium | high}
end
```

The default option of Medium at RC4 (128 bits) is acceptable, but the High option, AES (128/256 bits) and 3DES is more secure. The Low option, RC4 (64 bits), DES and higher does not meet PCI DSS requirements.

Protecting the CDE network from viruses

PCI DSS requires the use of regularly updated antivirus protection. The antivirus functionality of the FortiGate unit protects both the FortiGate unit and the networks it manages. Workstations on these networks can be protected using FortiClient Endpoint Security. Both FortiGate and FortiClient antivirus protection can receive updates from Fortinet's FortiGuard service. Workstations can also use third-party antivirus applications with update services.

The FortiGate unit can enforce the use of antivirus software, denying unprotected workstations access to the network.

Enabling FortiGate antivirus protection

The antivirus profile must apply AV scanning to all protocols. You also need to enable SSL inspection to include secure protocols in antivirus scanning. The extended AV database contains the largest number of virus signatures.

To enable SSL inspection

1. Go to **Security Profiles > SSL/SSH Inspection**.
2. Set **Inspection Method** to **Full SSL Inspection**.
3. Set each listed protocol to **On** and then select **Apply**.

To select the extended antivirus database

The antivirus database is selectable using the CLI:

```
config antivirus settings
   set default-db extended
end
```

For detailed information about the Antivirus feature, see the Security Profiles chapter of the FortiOS Handbook.

Configuring antivirus updates

On the dashboard, check the **License Information** widget. The **Support Contract** section should indicate that the FortiGate is registered and show future expiry dates for the FortiGuard Antivirus license. If your FortiGate unit is not registered, you can register it from the License Information widget.

In the **FortiGuard Services** section, check the **Antivirus** field. If the service is unreachable, see the online Help for information about troubleshooting your connectivity to FortiGuard Services.

Enforcing firewall use on endpoint PCs

PCI DSS requires you to “install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. (1.4)” Consider using the Endpoint Control feature of the FortiGate unit to enforce use of this software.

Monitoring the network for vulnerabilities

There are several tools that can assist you in monitoring your network for vulnerabilities and provide evidence to the PCI DSS auditor of such monitoring.

FortiGate logs

FortiGate units can be configured to send logs to FortiAnalyzer unit. In a larger network, this enables you to collect log information in a central location from several FortiGate units. You can also send logs to FortiCloud and to multiple syslog servers.

Monitoring with other Fortinet products

In addition to your FortiGate unit and its FortiOS firmware, there are several other Fortinet products that can assist your organization to comply with PCI DSS requirements.

Fortinet Database Security (FortiDB)

A FortiDB appliance or FortiDB software can provide vulnerability scanning and activity monitoring for your databases. For more information about this product, see the Fortinet website, www.fortinet.com.

FortiWeb Web Application Security

If your organization engages in e-Commerce, you can use FortiWeb Application Security to protect your web servers against attack. The FortiWeb application protects against HTTP and XML-based attacks, guards against attempts to deface your websites, and scans web servers for vulnerabilities. For more information about this product, see the Fortinet website, www.fortinet.com.

Restricting access to cardholder data

In addition to security policies and authentication governing access to the CDE, you can deploy the Fortinet Database Security (FortiDB) device, which provides vulnerability assessment, database activity monitoring, auditing and monitoring. You can also deploy FortiAuthenticator to increase authentication options.

Controlling access to the CDE network

PCI DSS requires each user to be uniquely identified and authenticated. On the FortiGate unit, this applies to administrators and to users of SSL VPN and IPsec VPNs.

Password complexity and change requirements

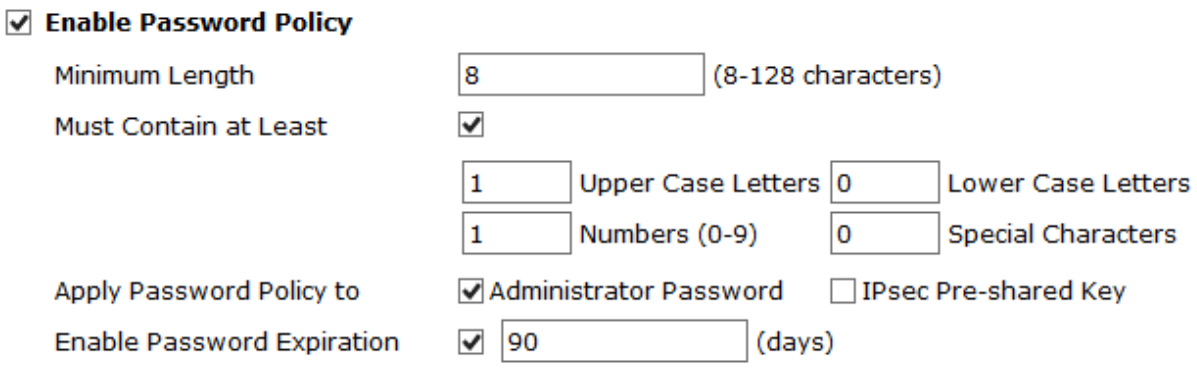
By default, the FortiGate unit admin account has no password. Be sure to define a password.

PCI DSS password requirements are:

- Require a minimum length of at least seven characters. (8.2.3)
- Contain both numeric and alphabetic characters. (8.2.3)
- Change user passwords/passphrases at least every 90 days. (8.2.4)

To facilitate creation of compliant administrator passwords, you can set a password policy. Go to **System > Settings** Select **Enable Password Policy**, enter the following and then select **Apply**.

The password policy does not apply to user passwords. Both password complexity and password expiry for users would need to addressed by making them a policy in your organization.



Minimum Length	8 or more. (Field does not accept a value less than 8.)
Must Contain	At minimum, set a required number of **Numerical Digits** and either **Upper Case Letters** or **Lower Case Letters**. Also setting a required number of **Non-alphabetic Letters** is acceptable.
Apply Password Policy to	Select **Administrator Password**.
Enable Password Expiration	Set to 90 days or less. The default is 90 days.

Password non-reuse requirement

PCI DSS requires that passwords are not re-used to satisfy the change requirement:

- Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. (8.2.5)

FortiGate users don't set their own passwords. The super_admin administrators can and so can admins with appropriate access. There is, however, no FortiGate-based mechanism to limit re-use of passwords.

Administrator lockout requirement

PCI DSS requires a user account lockout for administrators to guard against unauthorized access attempts:

- Limit repeated access attempts by locking out the administrator after not more than six attempts. (8.1.6),
- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (8.1.7)

You can meet these requirements with the following CLI commands:

```
config system global
   set admin-lockout-threshold 6
   set admin-lockout-duration 1800
end
```

The threshold can be less than 6 and the lockout duration can be more than 1800.

Administrator timeout requirement

PCI DSS requires:

- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. (8.1.8)

By default, the idle timeout is five minutes. You can go to **System > Settings** and change the **Idle Timeout** timeout to any value up to the permitted value of 15 minutes.

Administrator access security

To accommodate the requirement for unique identification of each user, the generic admin account should either be assigned to only one administrator or not used at all. You can create an administrator account for each administrator in **System > Administrators**.

You can also rename the admin administrator account to something that attackers are less likely to guess. To rename the admin administrator account you must go to **System > Administrators** and create a new administration account with the super_admin administrator profile and then login with this new account and change the name of the admin administrator account.

If an administrator always works from the same workstation, consider using the Trusted Host feature. The administrator will be able to log in only from a trusted IP address. You can define up to three trusted IP addresses per administrator.

Administrative access must also be enabled per network interface. Go to **Network > Interfaces** to edit the interface settings. Enable administrative access only on interfaces where you would expect the administrator to connect. Allow only secure connection protocols, HTTPS for web-based access, SSH for CLI access.

Remote access security

For remote access, PCI DSS requires two-factor authentication: a password and some other authentication, such as a smart token or certificate. This applies to employees, administrators, and third parties.

For remote access from the Internet, if possible you should also use the trusted hosts feature to limit the source addresses from which administrators can log into the FortiGate.

SSL VPN users

For SSL VPN users, implement two-factor authentication by requiring users to have a certificate in addition to the correct password. Go to **VPN > SSL-VPN Settings**, enable **Require Client Certificate**.

IPsec VPN users

If remote Users access your network using an IPsec VPN, you can implement two-factor authentication by adding a user group to a Remote Access IPSec VPN tunnel that requires two-factor authentication with FortiToken. This adds extended authentication (XAUTH) to the VPN and requires the user to use two-factor authentication in addition to the VPN authentication provided by the certificate or pre-shared key. As PCI DSS requires each user to have a unique identifier, you should already have user accounts and user groups defined.

FORTINET®

High Performance Network Security